IS SUPERVISION BY RISK

CHAPTER 2

(FILE NAME ON DISK # 1 = S1C2.WPD)

FFIEC member agencies supervise all financial institutions according to a philosophy based on providing high quality supervision. This supervision is directed at identifying existing or potential problems, and ensuring that problems are corrected. Because banking is essentially a business of accepting and managing risk, that philosophy is centered on evaluating risks. FFIEC member agencies apply that philosophy in all supervisory activities they conduct, including IS examinations.

Regulators must communicate with individual institutions and the industry to influence the change necessary to assess, monitor, and control risks appropriately.

Institution management is responsible for controlling risk. Regulatory agencies assess the quality of risk management, conducting oversight rather than audit. This type of supervision concentrates on systemic issues and institutions or areas that pose the greatest risk to the system.

FFIEC IS RISK OVERVIEW PROGRAM

Each FFIEC member agency maintains an IS regulatory program responsible for identification and reduction of unwarranted risks that could threaten a healthy system of financial institutions. The programs are supported by a small cadre of specially trained IS examiners who examine information systems and technology posing the greatest levels of transaction risk. IS examinations of institutions and independent vendors are designed to supplement other types of examinations (safety and soundness, compliance, fiduciary, etc.) of federally insured financial institutions. The timing and scheduling of IS examinations are determined by a number of factors including risk analysis results, inter-agency coordination at district and national levels, and intra-agency coordination with other types of examinations.

The IS regulatory program is based on the concept of Supervision by Risk. IS regulatory staff is directed by each agency's management to entities with high risk conditions or profiles (e.g. large, complex, or difficult to review information systems environment) affecting institutions under their jurisdiction. Supervision by Risk involves the selection of entities warranting examinations by IS examiners, followed by the development of a risk based supervisory strategy for each entity. This approach provides for analysis of examination coverage by IS examiners of all institutions and independent vendors in areas such as EFT switches, service bureaus, bill payment processors, software vendors, disaster recovery services, etc. Institutions, their independent vendors, and emerging risk areas are monitored and evaluated regularly by each agency's management for inclusion in the caseload for IS examiners.

RISK DEFINITION

Risk is the potential that events, either expected or unanticipated, may have an adverse impact on the institutions' or firms' earnings or capital. The existence of risk is not a reason for concern. Rather, examiners must determine if the risks are warranted. Generally, risks are warranted when they are: understandable, controllable, and within the institution's capacity to readily withstand adverse performance. When unwarranted risk occurs, whether deliberate or unintentional, examiners must communicate with management to mitigate risks by controlling or limiting exposure. Appropriate actions would normally include reducing exposures, strengthening controls, increasing capital, and ensuring the presence of an effective level of policies and procedures.

IS examiners primarily focus on transaction risk. These risks are associated with service or product delivery, and with providing support in all management processes (e.g., information for decision making and financial control). Transaction risk is present in all products, services, and aspects of an institution's operations (including at vendor locations). A major thrust of the IS examination is reviewing the effectiveness of management information systems and technology.

RISK ANALYSIS

An IS risk analysis assists examiners in developing a risk based supervisory strategy. This includes setting examination scope and objectives and identifying appropriate examination procedures necessary to support the overall strategy.

Time spent on examining areas should be commensurate with the level of risk that is present. Examiners will perform a risk analysis at least once during each supervisory cycle. An optional risk analysis form is located in the following workprogram. It describes one method that can be used in measuring and assessing risk.

Measuring and Assessing Risk

A common framework to document decisions about risk ensures effective supervision and consistency. Risk analysis is intended to provide examiners with a concise method of communicating and documenting judgments about the quantity of risk and quality of risk management and aggregate levels of risk. Risk assessments give both a current and prospective view of the institution's or independent vendor's risk profile.

The following approach for measuring and assessing risk is presented as an example and represents one such methodology. Each FFIEC member agency has the latitude to adopt policies or approaches representing different methods of risk analysis.

IS examiners must make judgments on the following as they affect transaction risk:

- *Quantity of Risk* – This refers to the level or volume of risk present. The assessment notes if the level of risk is high, moderate, or low.

- *Quality of Risk Management* – This refers to how well risks are identified, understood, and controlled. Assessments are weak, acceptable, or strong.

- *Aggregate Risk* – The assessment is a summary judgment incorporating both the quantity of risk and the quality of risk management. It allows the examiner to weigh the relative importance of each factor for a given institution and directs specific activities and resources for supervisory strategies. This is categorized as high, moderate, or low.

- *Direction* – This reflects the examiner's views on likely changes to the risk profile over the next supervisory cycle. Direction is expressed as decreasing, stable, or increasing. Decreasing indicates that the examiner anticipates, based on current information, the aggregate risk will decline over the next 12 months. Stable indicates the examiner anticipates the aggregate risk profile will remain unchanged. Decisions on the direction of risk may influence the supervisory strategy.

The institution's risk profile should guide the supervisory strategy and examiner resources employed.

Quantity of Risk

When assessing the quantity of risk, the IS examiner should consider:

- Transaction dollar exposure relative to earnings and capital of financial institutions.

- Transaction volume relative to the information system's capacity.

- Changes in ownership or management.

- The complexity of hardware and software systems and stability (current and projected) of these systems.

- The volume and risk exposure relative to the internal control exceptions.

- The potential for significant financial loss due to:
  - Human error or fraud.
  - Competitive disadvantage.
  - Incomplete information.
  - Operational disruption.

- The history of litigation relative to operations.

- The adequacy of controls over outsourcing arrangements.

- The examiner should also consider new activities that are not readily quantified (e.g., current emerging concepts with Internet activities.)

A review of those factors should allow the examiner to quantify the aggregate transaction risk to one of the following risk categories:

- **High** – The level of transaction processing and state of systems expose the institution or system of financial institutions to significant damage to reputation or loss of earnings or capital. The institution may have a history of transaction processing failures. The likelihood of future processing failures remains large because of the absence of effective internal controls.

- **Moderate** – The state of systems adequately supports the level of transaction processing. The volume and complexity of activities expose the institution to a degree of risk. Possible losses to reputation, earnings, or capital exist, but are mitigated by adequate internal controls.

- **Low** – The level and complexity of transaction processing is low and well supported by the state of systems development. Possible damage to reputation; loss of earnings; or capital is slight. The institution has a history of sound operations. The likelihood of future transaction processing failures is minimal in the presence of strong internal controls.

Quality of Risk Management

Risk analysis involves an assessment of the quality of risk management. Institutions successful in risk taking are those that have a corporate culture that balances controls and business initiatives. No single system works for all institutions, because conditions and organizational structures vary. Each institution should have its own risk management program tailored to its individual needs and circumstances. Sound risk management systems have several common fundamentals. For example, all risk management systems should be independent of risk-taking activities. Regardless of the risk management program's design, each should include:

- Risk Identification – Proper risk identification strives to recognize and understand existing risks or risks that may arise from new business initiatives. This should be a continuing process.

- Risk Measurement – Accurate and timely measurement of risks is critical to effective risk management systems. The lack of a risk measurement system inhibits the ability to limit or monitor risk levels. The sophistication of measurement tools should be suited to the complexity and levels of risk assumed. Periodic tests should be performed to validate the integrity of the measurement tools.

- Risk Control – Limits should be established and communicated through policies, standards, or procedures that define responsibility and authority. These control limits should be meaningful management tools that may be adjusted to changes in conditions or risk tolerances. A process should exist to authorize and monitor exceptions to risk limits when warranted.

- Risk Monitoring – Risk levels should be monitored to ensure timely review of risk positions and exceptions. Reports should be frequent, timely, accurate, and informative and should be distributed to appropriate persons to ensure action.

Effective risk management is more than merely a process comprised of those controls. It requires an informed board, capable management, and appropriate staffing. The board must guide the institution's strategic direction by approving policies that endorse the organization's risk tolerance. Well designed monitoring systems allow the board to hold management accountable for operating within established tolerance levels.

Capable management and appropriate staffing are critical to effective risk management. Institution management is responsible for the implementation, integrity, and maintenance of risk management systems. Management must also keep the directorate adequately informed. In discharging its role, management:

- Implements the company's strategic direction.

- Defines the institution's risk tolerance through the development of policies that are compatible with strategic goals.

- Develops management information systems that are timely, accurate, and informative.

- Ensures that strategic direction and risk tolerance are communicated effectively throughout the organization.

Examiners assess risk management systems by considering policies, processes, personnel, management, and control systems. A significant deficiency in one or more constitutes a deficiency in risk management. Uncorrected, the deficiency could affect adversely the institution's earnings, capital, or standing in the community by reflecting poorly on its intent, commitment, and ability to perform.

Examiners assess the quality of risk management by considering:

Whether policies are:

- Comprehensive, including whether they:

– Establish responsibilities and accountability.
– Set standards for systems development, changes,

– Provide for contingency planning.

- Consistent with strategic direction and risk tolerance levels.
- Approved by the board or an appropriately delegated committee, as necessary.

Whether a process exists for:

- Communicating related policies and expectations to appropriate personnel.

- Approving and monitoring compliance with policy limits.

- Responding to changing market conditions.

- Identifying information needs to manage the corporation efficiently.

- Defining the systems architecture for transaction processing and for delivering products and services.

- Developing and maintaining systems for product and service delivery.

- Monitoring system capacity and performance.

- Assuring the integrity and security of systems and the independence of operating staff.

- Documenting system (programming) history adequately.

- Assuring the reliability and retention of information (e.g., data creation, processing, storage, and delivery). This includes business continuity planning.

- Establishing effective internal administrative and accounting controls.

- Undertaking due diligence assessments.

- Ensuring the adequacy of controls over outsourcing arrangements.
- Providing the timely production and use of management information.

Whether personnel:

- Understand strategic direction, risk tolerance limits, and policies.
- Exhibit technical and/or managerial competency in relation to the complexity of products.

- Are sufficient in number and skills for current and anticipated needs.

- Are adequately compensated so that turnover is limited and stability fostered.

Whether management:

Demonstrate a commitment to training, development, and continuing education programs.

- Demonstrate a commitment to providing an effective performance management program.

- Ensure independence, expertise, and competency in performing control functions, such as loan review or audit.

Whether control systems are designed to provide:

- Timely, accurate, and meaningful management information.

- Independent and effective feedback on compliance with policies and operating procedures. Control systems should be consistent with the complexity of the activities, but, at a minimum, should include internal and/or external audit reviews.

A review of those factors should allow examiners to assess and rate the quality of transaction risk management in an institution. The rating, described as weak, acceptable, or strong according to the following guidelines, should be incorporated as appropriate into the overall rating for management.

- **Weak** – Responsible officials do not understand, or have chosen to ignore, key aspects of transaction risk. Management does not anticipate or take prompt or appropriate actions in response to changes in the market or technology. Policies to control transaction risk do not exist or are inadequate. Serious weaknesses exist in operating and information systems, internal controls, internal and external audit coverage, or contingency plans. Management information on transaction processing activities exhibits significant weaknesses. Planning or due diligence may be inadequate, allowing exposure to risk by introducing new products and services or acquisitions. There may be exposure to processing risks due to poor conversion management, either from integration of new acquisitions with existing systems, or from converting one system to another. Management has not demonstrated a commitment to make the corrections required to improve transaction processing risk controls.

- **Acceptable** – Responsible officials reasonably understand the key aspects of transaction processing risk. Management responds adequately to changes in the market or technology. Management identifies and measures the most significant processing risks. Policies exist that address exposure to significant processing risks. Procedures may contain only modest deficiencies. Adequate operating and information processing systems, internal controls, audit coverage, and contingency plans are evident. Minor deficiencies may exist in management information that relates to transaction and information processing activities.

- **Strong** – Responsible officials fully understand all aspects of transaction processing risk. Management anticipates and responds well to changes of a business, economic, market or technological nature that affect processing risk. Management has comprehensive policies addressing transaction processing risks. Implementation plans are clear and followed. Systems, internal controls, audit and contingency plans are sound. Management has demonstrated favorable performance in acquisitions and the introduction of new products and services. Management identifies weaknesses quickly and takes appropriate action.

SUPERVISORY STRATEGIES

A supervisory strategy is a plan to provide effective, efficient supervision for each organization. Those dynamic documents are reviewed and updated regularly based on the organization, industry, and economic developments. The following optional workprogram may help provide guidance for the development of a supervisory strategy. Each FFIEC member agency is responsible for the development of its own policies on developing risk based supervisory strategies.

The IS EIC prepares the strategy which is reviewed subsequently by the next higher level of management. The supervisory strategy directs examination activities and is based on:

- Statutory and policy based examination requirements.

- Agency standards and priorities.

- Knowledge of the institution including:

– Risk profile.
– Strengths and weaknesses.
– Supervisory history.
– Market factors.

Elements of a Supervisory Strategy

The three primary elements of the supervisory strategy are:

Objectives – Document the EIC's goals for supervision of the institution based on its risk profile and appropriate statutory or agency standards. They are the foundation for all activities and work plans. Well defined objectives provide for focused and efficient examination activities and help managers ensure consistent and appropriate application of supervisory policy. Supervisory objectives must be clear, attainable, specific, and action-oriented.

Activities – Detail steps that will achieve supervisory objectives. Each activity should link directly to one or more of the supervisory objectives. They should be focused on ensuring that risk management systems operate effectively. Activities should include a plan for communication with the institution, detailing the types and frequency (e.g., report of examination, meeting with the board of directors, etc.)

Work plans – Include methods for achieving strategies. They provide details that outline the scope, timing, and resources needed to meet supervisory objectives and strategies.